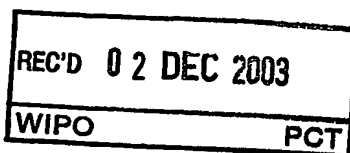




10/537838

ST/IB 03 / 0 5 3 4 3
2 1. 11. 03

INVESTOR IN PEOPLE



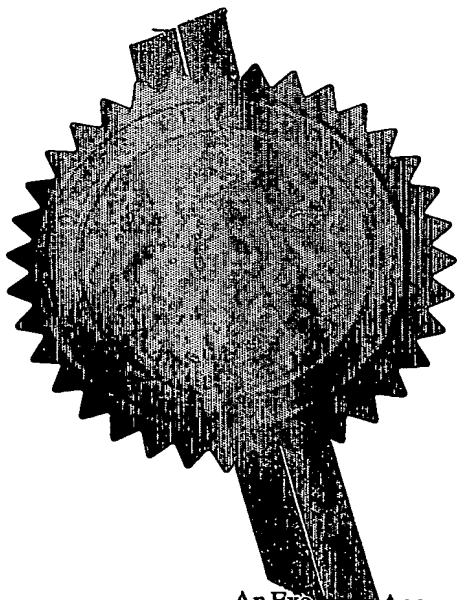
The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.



Signed

H. Behen

Dated

10 September 2003

**PRIORITY
DOCUMENT**

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

BEST AVAILABLE COPY

The
Patent
Office11D E769971-2 002879
P01/7700 0.00-0228808.2

1/77

Request for grant of a patent

(See notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

THE PATENT OFFICE
M

11 DEC 2002

NEWPORT

The Patent Office
Cardiff Road
Newport
Gwent NP10 8QQ

Your reference

PHGB020217

Patent application number

(The Patent Office will fill in this part)

0228808.2

11 DEC 2002

Full name, address and postcode of the or of
each applicant (underline all surnames)KONINKLIJKE PHILIPS ELECTRONICS N.V.
GROENEWOUDSEWEG 1
5621 BA EINDHOVEN
THE NETHERLANDS
07419294001

Patents ADP Number (if you know it)

If the applicant is a corporate body, give the
country/state of its incorporation

THE NETHERLANDS

Title of the invention

METHOD AND APPARATUS FOR MEASURING DISTANCE

Name of your agent (if you have one)

"Address for service" in the United Kingdom
to which all correspondence should be sent
(including the postcode)Philips Intellectual Property and Standards
Cross Oak Lane
Redhill
Surrey RH1 5HA
08359655001 ✓

Patents ADP number (if you know it)

If you are declaring priority from one or more
earlier patent applications, give the country
and the date of filing of the or of each of these
earlier applications and (if you know it) the or
each application number

Country

Priority Application number.
(if you know it)Date of filing
(day/month/year)If this application is divided or otherwise
derived from an earlier UK application, give
the number and the filing date of the earlier
application

Number of earlier application

Date of filing
(day/month/year)Is a statement of inventorship and of right to
grant of a patent required in support of this
request? (Answer "Yes" if:

YES

- a) any applicant named in part 3 is not an inventor, or
 - b) there is an inventor who is not named as an
applicant, or
 - c) any named applicant is a corporate body.
- See note (d))

9. Enter the number of sheets for any of the following items you are filing with this form.
Do not count copies of the same document.

Continuation sheets of this form

Description
Claims(s)
Abstract
Drawings

9 ✓
4 ✓
1 ✓
3 only ✓

10. If you are also filing any of the following, state how many against each item:

Priority Documents

Translations of priority documents

Statement of inventorship and right

to grant of a patent (*Patents Form 7/77*)

Request for preliminary examination and
search (*Patents Form 9/77*)

Request for substantive examination
(*Patents Form 10/77*)

Any other documents

(*Please specify*)

11.

I/We request the grant of a patent on the basis of this application

Signature

P. J. Mabey

Date

10/12/02

12. Name and daytime telephone number of person to contact in the United Kingdom

01293815576

(Peter J Mabey)

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

- If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.*
- Write your answers in capital letters using black ink or you may type them.*
- If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.*
- If you have answered "Yes" Patents Form 7/77 will need to be filed.*
- Once you have filled in the form you must remember to sign and date it.*
- For details of the fee and ways to pay please contact the Patent Office.*

DESCRIPTION

METHOD AND APPARATUS FOR MEASURING DISTANCE

5 The invention relates to a method and apparatus for use in the measurement of distance.

Wireless devices which measure their proximity to another device, or their absolute position, are becoming more widespread. They are increasingly
10 being used in applications where security is an issue. One example is a child locator device which enables a parent to keep track of the whereabouts of their child. A second example is a passive keyless entry system for vehicles, in which the proximity of the owner with a key fob in his pocket is sufficient to trigger the vehicle to unlock its doors. A third example is a wireless tag that
15 can be attached to an object to monitor its whereabouts and to detect unauthorised movement. In these examples, the system must be robust against attack, in the case of the first example, from a child abductor, or indeed an ingenious child who doesn't wish to be tracked, and in the case of the other examples, a thief.

20 One technology that can be used for proximity detection over a local area is described in "Designing a positioning system for finding things and people indoors", J.Werb and C. Lanzl, IEEE Spectrum, September 1998. In this article Werb et al describe a system in which a signal is sent from a master unit to a tag being carried on the person being tracked. The tag receives the
25 signal and simply re-transmits the signal on a different frequency without processing it. The master unit measures the time-of-arrival of the returning signal, compares it with the time at which it transmitted the signal to the tag and calculates the range to the tag.

30 Such a known technology is open to attack by a third party or by one of the parties involved in the proximity measurement who wishes to lie about their whereabouts. The attack can comprise inserting an additional delay so that an artificially long time-of-arrival is measured and consequently the tag appears to

be further away from the master unit than it actually is. Adding such a delay might be a relatively simple procedure: for example, in a system with a screw-in antenna, an extra delay element such as an off-the-shelf microwave filter could be screwed in between the antenna and the device. The tag itself will introduce some delay, since it cannot instantaneously re-transmit the signal. This inherent delay can be calibrated out at the factory during manufacture.

Other known technologies use a signal generated and transmitted from the tag, rather than using the tag as a transponder, although the transmission from the tag may be initiated by receipt of a signal sent from the master unit. Such systems are also vulnerable to attack by insertion of additional delay.

An attack may also result in the tag appearing to be closer to the master unit than it actually is. This is because, in order to permit a simple detection circuit, the signal used for making the range measurement typically comprises a repeated code sequence. As a result there is an ambiguity in the time-of-arrival equal to multiples of the duration of the code, and consequently an ambiguity in the measured range. So, for example, a code sequence having a duration of $10\mu\text{s}$ results in an ambiguity in the time-of-arrival equal to $n \times 10\mu\text{s}$, where n is any integer including zero. Consequently there is an ambiguity in the measured range of $n \times 3\text{km}$, so the master unit cannot differentiate between a tag at, say, 10m and 3010m . Therefore a tag at a distance of 3010m may appear to be 10m from the master unit. Of course a signal received over a distance of 3010km would be attenuated compared with a signal received over 10m , but an attacker may readily compensate for this attenuation by boosting the signal level.

The attack by insertion of additional delay is illustrated by the timing diagram in Figure 1. Figure 1 a) illustrates the signal being transmitted from a master unit at time t_0 . The signal is a Direct-Sequence Spread-Spectrum (DSSS) signal comprising a repeated spreading code 10 which begins with binary chips '10011' and has a duration t_p . Figure 1 b) illustrates the signal received back at the master unit at time t_1 having been received and re-transmitted by a tag. The genuine round-trip delay $t_1 - t_0$ measured at the

master unit comprises the genuine time-of-flight to the tag and back again, and the delay inherent in the tag. Figure 1 c) illustrates the signal 20 which might be received at time t_2 when the system is under attack. The attacker has inserted an extra delay $\delta = t_2 - t_1$ so that the total round-trip time exceeds one code period t_p . The master unit cannot tell the difference between the signal 20 received at time t_2 and a hypothetical signal 30 received at $t_2 - t_p$ and measures the round-trip delay as $\Delta = t_2 - t_p - t_0$, which is much shorter than the genuine round-trip delay. Consequently the tag appears to be much closer to the master unit than it actually is. The attacker may make the apparent distance take any desired value by appropriate selection of the additional delay δ .

The attack by insertion of additional delay may be implemented by tampering with the tag, or may be implemented as a relay attack. In a relay attack, the attacker uses an intermediate device to relay signals from the tag to the master unit, and also from the master unit to the tag if required. By inserting, at the intermediate device, an appropriate delay into the signal, a distant tag may appear to be close to the master unit. Such a relay attack has been used by car thieves to deceive a car security system into unlocking the car doors when the owner with a passive keyfob is distant from his car.

The ambiguity problem could be avoided if a long codes is used and not repeated during the signal transmission, but such long codes result in a relatively complex receiver.

An object of the invention is to improve the robustness of distance measurement against attack.

According to a first aspect of the invention there is provided a method of determining a distance between a first device and a second device, comprising, at the first device, transmitting a signal comprising simultaneous first and second components, wherein the first component comprises a repeated first code and the second component comprises a repeated second code and the first and second codes are of unequal duration, and at the

second device: receiving the signal; detecting the first and second codes; determining from the detected first and second codes respective first and second indications of the distance; comparing the first and second indications of the distance; and generating a third indication of the distance in response to the first and second indications of the distance being equal within a predetermined tolerance.

According to a second aspect of the invention there is provided a system for determining distance comprising a first device having means for transmitting a signal comprising simultaneous first and second components, wherein the first component comprises a repeated first code and the second component comprises a repeated second code and the first and second codes are of unequal duration, and a second device having means for receiving the signal, means for detecting the first and second codes, means for determining from the detected first and second codes respective first and second indications of the distance, means for comparing the first and second indications of the distance, and means for generating a third indication of the distance in response to the first and second indications of the distance being equal within a predetermined tolerance.

According to a third aspect of the invention there is provided a device for determining distance, comprising means for receiving a signal comprising simultaneous first and second components, wherein the first component comprises a repeated first code and the second component comprises a repeated second code and the first and second codes are of unequal duration, means for detecting the first and second codes, means for determining from the detected first and second codes respective first and second indications of the propagation distance of the signal, means for comparing the first and second indications of the propagation distance, and means for generating a third indication of the propagation distance in response to the first and second indications of the propagation distance being equal within a predetermined tolerance.

According to a fourth aspect of the invention there is provided a device suitable for use in a system for measuring distance, comprising means

for generating and transmitting a signal comprising simultaneous first and second components, wherein the first component comprises a repeated first code and the second component comprises a repeated second code and the first and second codes are of unequal duration.

5 By using a signal comprising simultaneous codes having different durations, it becomes more difficult for an attacker to detect the signal. Therefore the system is more robust against attack.

By using a signal comprising simultaneous codes having different durations, performing separate distance measurements using each code, and
10 requiring each measurement to yield the same or a similar result, it becomes more difficult for an attacker to implement an additional delay which will deceive the system. Therefore robustness is further improved.

In general, when using a signal comprising simultaneous, repeated codes having different durations, the additional delay which should be
15 introduced by an attacker to successfully deceive the system is a common multiple of the durations of the constituent codes. By selecting the code durations such that the least common multiple (LCM) duration corresponds to a time-of-flight, and hence distance, that can readily be discounted as false, the system can be even more robust against attack. For example, consecutive
20 measurements made a short time interval apart but indicating widely differing distances may indicate an impossible speed of motion, and therefore indicate that the system has been subject to attack.

Preferably, the respective durations of the first and second codes are proportional to respective numbers having a relative prime relationship. Such
25 a relationship results in a least common multiple (LCM) duration which is long, thereby improving robustness against attack.

Optionally, the signal transmitted by the first device may be a re-transmission of a signal received by the first device, having been transmitted initially by the second device.

30

The invention will now be described, by way of example only, with reference to the accompanying drawings wherein:

Figure 1 is a timing diagram illustrating attack by insertion of additional delay,

Figure 2 is a schematic block diagram of a system for measuring distance,

5 Figure 3 is a schematic block diagram of a device for determining distance,

Figure 4 is a schematic block diagram of a device for use in a system for measuring distance,

10 Figure 5 is a schematic block diagram of an alternative embodiment of a device for use in a system for measuring distance, and

Figure 6 is a schematic block diagram of a further alternative embodiment of a device for use in a system for measuring distance.

Referring to Figure 2, there is shown a system for measuring distance
15 comprising a first device 100 and a second device 200. The first device 100 could be, for example, a tag attached to a parcel, and the second device 200 could be a master unit for tracking parcels. As a further example, the first device 100 could be a keyfob and the second device 200 could be a vehicle security unit. In operation a signal is transmitted from the second device 200,
20 is received by the first device 100 and is re-transmitted back to the second device 200 on a different frequency where it is received and processed to determine the distance between the first device 100 and the second device 200.

Referring to Figure 3, there is shown a schematic block diagram of the
25 second device 200. There is a first code generator 210 comprising a first linear feedback shift register for generating a first code and a second code generator 215 comprising a second linear feedback shift register for generating a second code. The first and second codes comprise a different number of chips, denoted respectively N_1 and N_2 , but a common chip rate,
30 which results in the first and second codes having different durations. Alternatively, the first and second codes can comprise a common number of

chips but different chip rates, denoted respectively C_1 and C_2 , which also results in the first and second codes having different durations.

In operation, the first code generator 210 generates a first signal component comprising the first code repeated identically, and the second code generator 215 generates simultaneously a second signal component comprising the second code repeated identically. The first and second code generators 210, 215 are coupled to a clock 218 for controlling the time of generation and the rate of generation of the first and second codes.

An output from each of the first and second code generators 210, 215 is coupled to respective inputs of a summing means 220 for summing the first and second signal components, and an output from the summing means 220 is coupled to an input of a transmitter 230 for transmitting a signal comprising a carrier modulated with the first and second signal components. An output of the transmitter 230 is coupled to an antenna 250 by means of a circulator 240.

The antenna 250 is coupled via the circulator 240 to an input of a receiver 260 for receiving the transmitted signal after it has been received and re-transmitted by the first device 100. An output of the receiver 260 is coupled to an input of a first code detector 270 for detecting the first code and to an input of a second code detector 275 for detecting the second code. The first and second code detectors 270, 275 are adapted to correlate the received signal with stored reference copies of respectively the first and second codes, and to measure the time-of-flight of each of the detected first and second codes. The first and second code detectors 270, 275 are coupled to the clock 218 which provides them with a timing reference to enable time-of-flight to be determined.

An output from each of the first and second code detectors 270, 275 is coupled to a comparison means 280 for comparing the respective time-of-flight measurements made by the first and second code detectors 270, 275. If the two time-of-flight measurements are equal within a predetermined tolerance, the comparison means 280 converts the time-of-flight into a distance value and delivers the distance value on a first output 281 to an application processor 290 for further processing dependent on the specific application. For example,

if the application is a vehicle security system, the application processor 290 may be adapted to unlock a vehicle door if the distance value is below a predetermined threshold value, indicating that the owner with the keyfob is close to the vehicle. As another example, if the application is a parcel tracking system, the application processor 290 may initiate an alarm if the distance value is above a predetermined threshold value, indicating that a parcel carrying the first device 100 is being moved without authorisation.

If the two time-of-flight measurements are not equal within the predetermined tolerance, the comparison means 280 issues an indication to the application processor 290 on a second output 282 that the system for measuring distance is under attack. The manner in which this indication is processed by the application processor 290 is dependent on the specific application and the indication could be, for example, simply ignored.

Referring to Figure 4, there is shown a schematic block diagram of the first device 100. There is a receiver 160 coupled to receive a signal from an antenna 150 via a circulator 140. An output of the receiver is coupled to an input of a transmitter 130, and the transmitter 130 is coupled to the antenna 150 via the circulator 140 to re-transmit the received signal on a different frequency.

In a preferred embodiment, the code lengths N_1 and N_2 have a relative prime relationship. Such a relationship may be implemented, for example, by using in the first code generator 210 a linear feed-back shift register having M stages arranged to generate a maximal length code having length $N_1 = 2^M - 1$ chips, and using in the second code generator 215 a linear feed-back shift register having $M+1$ stages arranged to generate a maximal length code having length $N_2 = 2^{(M+1)} - 1$ chips. Alternatively, the code chip rates C_1 and C_2 may have a relative prime relationship.

In an alternative embodiment, instead of the first device 100 retransmitting the signal received from the second device 200, the signal may be generated and transmitted by the first device 100. An embodiment of such a first device 100 is illustrated in Figure 5 and comprises the following elements equivalent to the indicated elements described above in relation to

the second device; first and second code generators 310, 315 (as 210, 215), clock 318 (as 218), summing means 320 (as 220), transmitter 330 (as 230), and antenna 350 (as 250). A corresponding embodiment of the second device 200 is as described above with reference to Figure 3, but with the first and second code generators 210, 215, the summing means 220, and the transmitter 230 omitted. Alternative, known means of synchronising the clocks 218 are incorporated into the first and second devices 100, 200.

Optionally, a common modulation scheme need not be used for both the first and second components of the signal. For example, one of the components may be frequency or phase modulated onto a carrier forming a Direct Sequence Spread Spectrum (DSSS) signal and the other component a low-bandwidth amplitude modulated carrier which occupies nulls in the DSSS spectrum.

Optionally, the signal may be generated using a quadrature modulator. Referring to Figure 6, a first mixer 410 multiplies the first component generated by the first code generator 310 by an in-phase local oscillator signal generated by a local oscillator 420 and a second mixer 430 multiplies the second component generated by the second code generator 320 by a quadrature-phase local oscillator signal. The resulting products are summed in the summing means 320.

Although the invention has been described in respect of a signal comprising simultaneous first and second components, the use of more than two simultaneous components is not excluded.

In the present specification and claims the word "a" or "an" preceding an element does not exclude the presence of a plurality of such elements. Further, the word "comprising" does not exclude the presence of other elements or steps than those listed.

From reading the present disclosure, other modifications will be apparent to persons skilled in the art. Such modifications may involve other features which are already known in the art of distance measurement and the art of signalling and which may be used instead of or in addition to features already described herein.

CLAIMS

1. A method of determining a distance between a first device and a
5 second device, comprising,
at the first device,
transmitting a signal comprising simultaneous first and second
components, wherein the first component comprises a repeated first
code and the second component comprises a repeated second code
10 and the first and second codes are of unequal duration, and
at the second device:
receiving the signal;
detecting the first and second codes;
determining from the detected first and second codes respective first
15 and second indications of the distance;
comparing the first and second indications of the distance; and
generating a third indication of the distance in response to the first and
second indications of the distance being equal within a predetermined
tolerance.
20
2. A method as claimed in claim 1, wherein the respective durations
of the first and second codes are proportional to respective numbers having a
relative prime relationship.
- 25 3. A method as claimed in claim 1 or 2, further comprising
transmitting the signal from the second device and at the first device receiving
the signal transmitted from the second device, wherein the transmitting at the
first device comprises retransmitting the signal received from the second
device.

4. A method as claimed in claim 1, 2 or 3, wherein at least one of the first and second indications of distance is an indication of time of flight of the signal.

5 5. A system for determining distance comprising
a first device having
means for transmitting a signal comprising simultaneous first and
second components, wherein the first component comprises a repeated
first code and the second component comprises a repeated second
10 code and the first and second codes are of unequal duration, and
a second device having
means for receiving the signal,
means for detecting the first and second codes,
means for determining from the detected first and second codes
15 respective first and second indications of the distance,
means for comparing the first and second indications of the distance,
and
means for generating a third indication of the distance in response to
the first and second indications of the distance being equal within a
20 predetermined tolerance.

6. A system as claimed in claim 5, wherein the respective durations
of the first and second codes are proportional to respective numbers having a
relative prime relationship.

25

7. A system as claimed in claim 5 or 6, the second device further
comprising means for generating and transmitting the signal, and the first
device further comprising means for receiving the signal transmitted by the
second device and wherein the means for transmitting is coupled to retransmit
30 the signal received from the second device.

8. A system as claimed in claim 5, 6 or 7, wherein at least one of the first and second indications of distance is an indication of time of flight of the signal.

5 9. A device for determining distance, comprising
means for receiving a signal comprising simultaneous first and second
components, wherein the first component comprises a repeated first code and
the second component comprises a repeated second code and the first and
second codes are of unequal duration,
10 means for detecting the first and second codes,
means for determining from the detected first and second codes respective
first and second indications of the propagation distance of the signal,
means for comparing the first and second indications of the propagation
distance, and
15 means for generating a third indication of the propagation distance in response
to the first and second indications of the propagation distance being equal
within a predetermined tolerance.

20 10. A device as claimed in claim 9, comprising means for generating
and transmitting the signal.

11. A device as claimed in claim 10, wherein the respective durations
of the first and second codes are proportional to respective numbers having a
relative prime relationship.

25

12. A device suitable for use in a system for measuring
distance, comprising means for generating and transmitting a signal
comprising simultaneous first and second components, wherein the first
component comprises a repeated first code and the second component
30 comprises a repeated second code and the first and second codes are of
unequal duration.

13. A device as claimed in claim 12, wherein the respective durations of the first and second codes are proportional to respective numbers having a relative prime relationship.

5 14. A device as claimed in claim 12 or 13, wherein the means for generating and transmitting the signal comprising simultaneous first and second components further comprises means for multiplying the first component by an in-phase local oscillator signal, means for multiplying the
10 for summing the resulting products.

ABSTRACT

METHOD AND APPARATUS FOR MEASURING DISTANCE

5 A device (200) measures distance using a wireless signal that comprises two simultaneously transmitted components. Each of the two components comprises a respective repeated code, the two codes having different durations. On receipt of the signal, the propagation distance is calculated separately for each code and compared (280). The calculated distance is
10 considered to be valid only if the two calculations yield the same result. Preferably the durations of the two codes are proportional to numbers having a relative prime relationship. The signal may be generated and transmitted by the same device (200) that performs the distance calculation, with the signal being retransmitted back to the device by a remote device (100), or may be
15 generated and transmitted by the remote device (100).

(Figure 3)

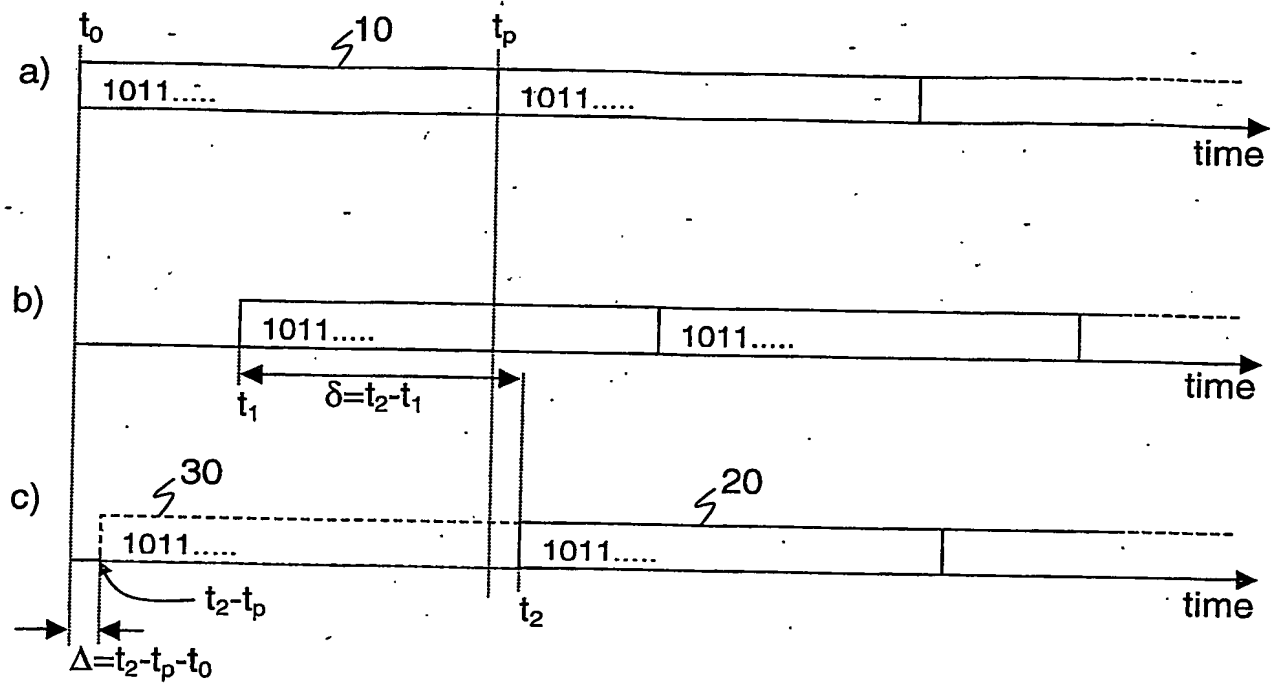


Fig.1

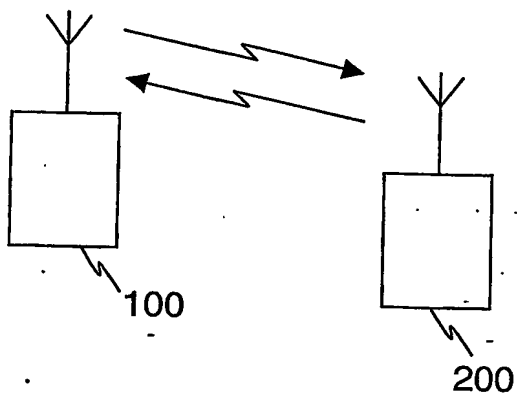


Fig.2

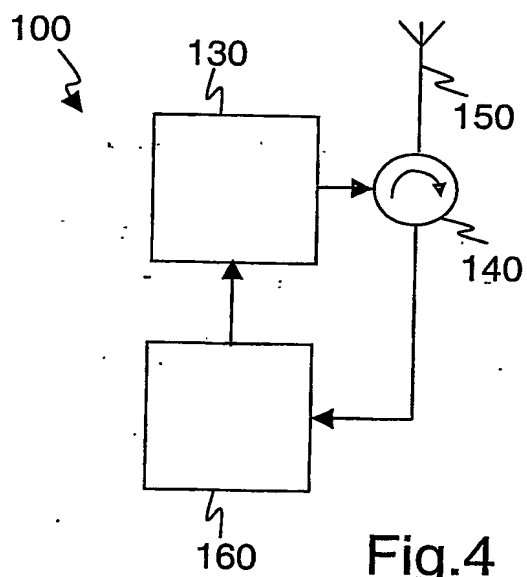


Fig.4

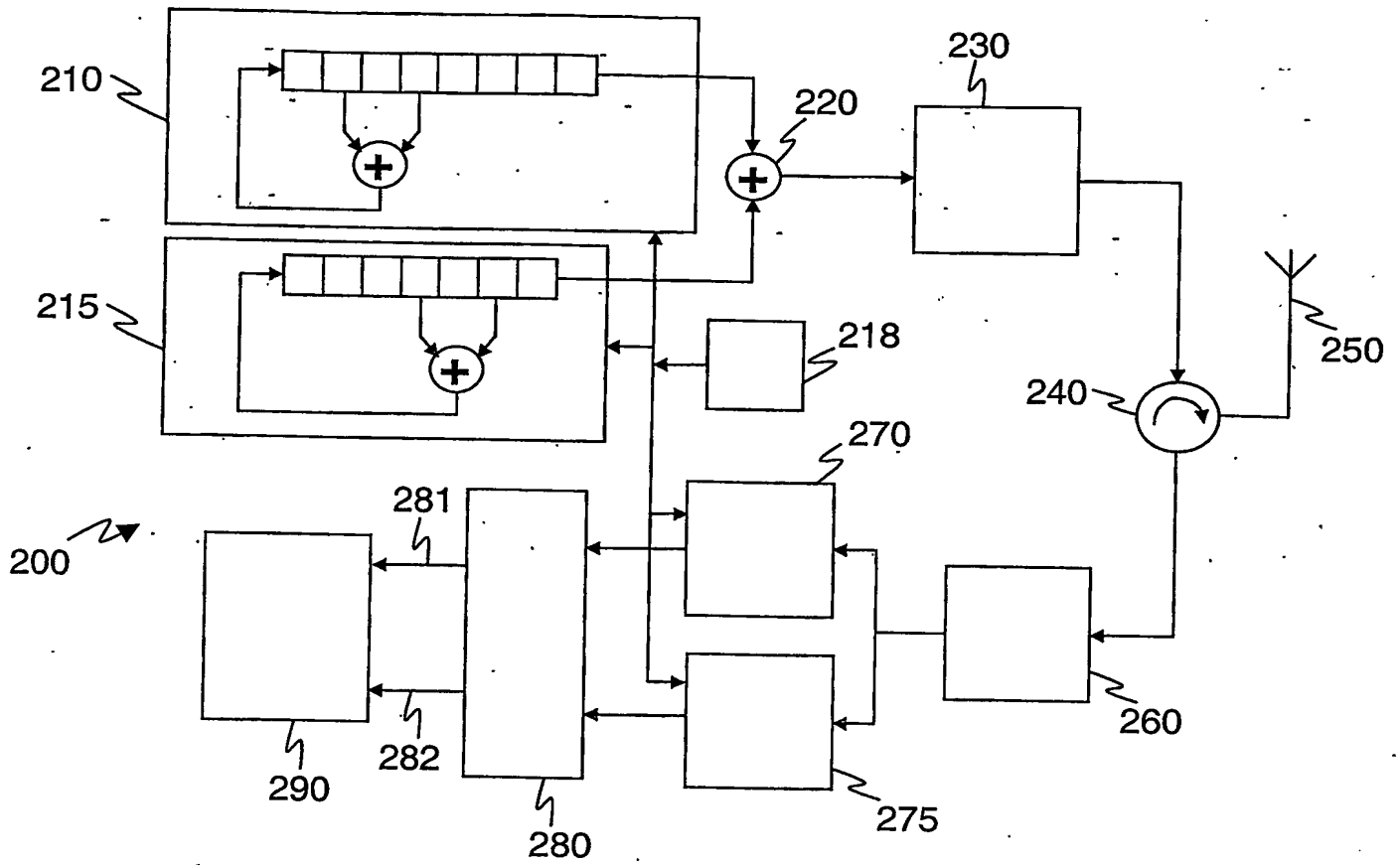


Fig.3

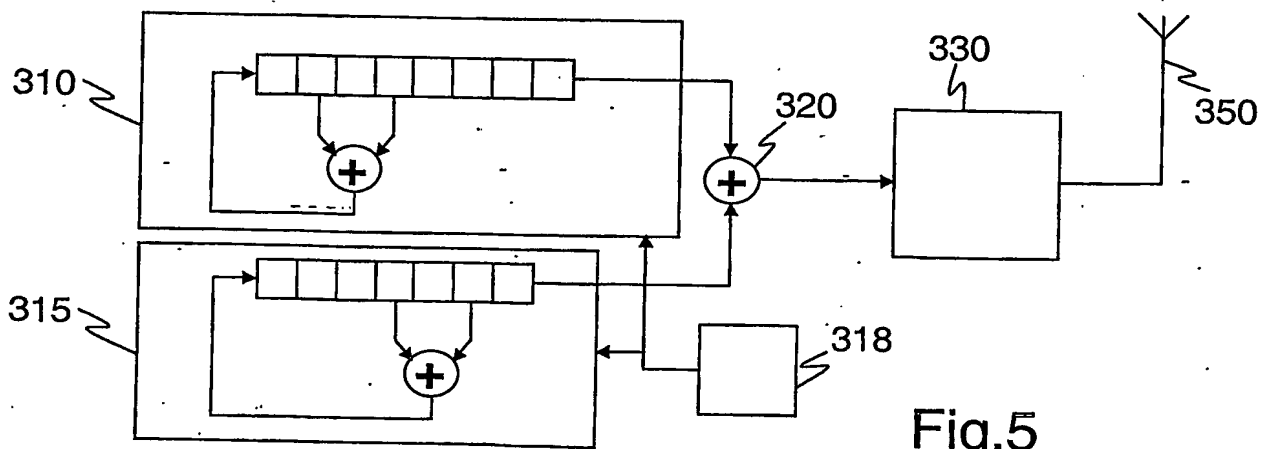


Fig.5

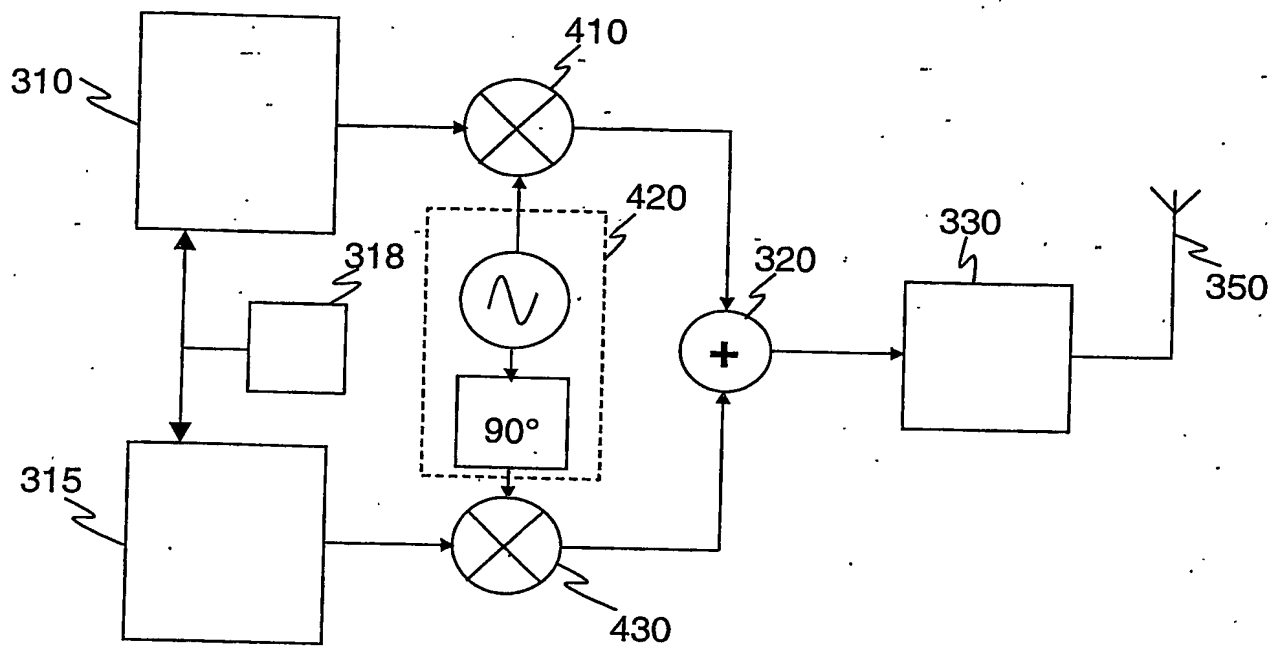
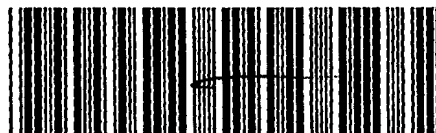


Fig.6

PCT Application
IB0305343



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☒ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☒ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.